Titre : Exemples d'extensions galoisiennes de degré 24 sur $\mathbb{Q}$

Auteur(s) : Nicolas Bureau

Revue : CaMUS (Cahiers Mathématiques de l'Université de Sherbrooke)

Volume : 3

Année : 2012

Pages : 70-79

Éditeur : Université de Sherbrooke. Département de Mathématiques

URI : Repéré à : http://camus.math.usherbrooke.ca/revue.html

Page vide laissée intentionnellement

CaMUS **3**, 70 – 79

Exemples d'extensions galoisiennes de degré 24 sur $\mathbb{Q}$

Nicolas Bureau

Résumé Le théorème fondamental de la théorie de Galois permet de donner la liste des sous-corps d'une extension algébrique de $\mathbb{Q}$ en utilisant la liste des sous-groupes de son groupe de Galois. L'objet de cet article est de décrire les sous-corps d'une classe d'extensions de degré 24 sur le corps $\mathbb{Q}$ des rationnels.

1 Introduction

Cet article tient pour acquis que la lectrice et le lecteur soient familiers avec la théorie des groupes ainsi qu'avec la théorie des extensions de corps.

La théorie de Galois est très utile dans plusieurs sphères des mathématiques telles que l'arithmétique ainsi que l'algèbre. Le théorème fondamental de cette théorie est inévitable lorsque vient le moment de faire l'éventail des sous-corps d'une extension donnée de $\mathbb{Q}$. En effet, elle permet de passer d'un problème *a priori* continu à un problème discret, celui des sous-groupes d'un groupe. Ce changement transforme la chasse aux sous-corps en une chasse aux sous-groupes.

Le but de cet article est de mettre la lumière sur un exemple d'application du théorème fondamental de la théorie de Galois [DF04]. Il s'agit d'étudier la classe d'extensions de la forme $\mathbb{Q}\left(\omega,\theta,\xi\right)/\mathbb{Q}$ où

$$\omega = \sqrt[6]{M}, \quad \zeta = \frac{1}{2}(1+\theta), \quad \theta = \sqrt{-3}, \quad \xi = \sqrt{m},$$

avec M et m deux entiers copremiers > 1 sans facteur carré et ζ une sixième racine primitive de l'unité. Dès maintenant, nous pouvons remarquer que $\mathbb{Q}(\omega,\theta,\xi)$ est une extension de degré 24 sur $\mathbb{Q}$. En effet,

$$[\mathbb{Q}(\omega,\theta,\xi):\mathbb{Q}] = [\mathbb{Q}(\omega,\theta,\xi):\mathbb{Q}(\theta,\xi)]\times[\mathbb{Q}(\theta,\xi):\mathbb{Q}(\xi)]\times[\mathbb{Q}(\xi):\mathbb{Q}] = 6\times2\times2 = 24.$$

Nous verrons dans les pages qui suivent que le diagramme de Hasse des sous-corps de $\mathbb{Q}(\omega,\theta,\xi)$ a l'allure de la Figure 19.

L'auteur tient à remercier son directeur de maîtrise, monsieur Claude Levesque, de l'Université Laval, sans qui cet article n'aurait jamais vu le jour. Ses nombreux conseils ainsi que son support financier sont grandement appréciés. L'auteur tient également à remercier le département de mathématiques de l'Université Laval pour sa contribution monétaire.

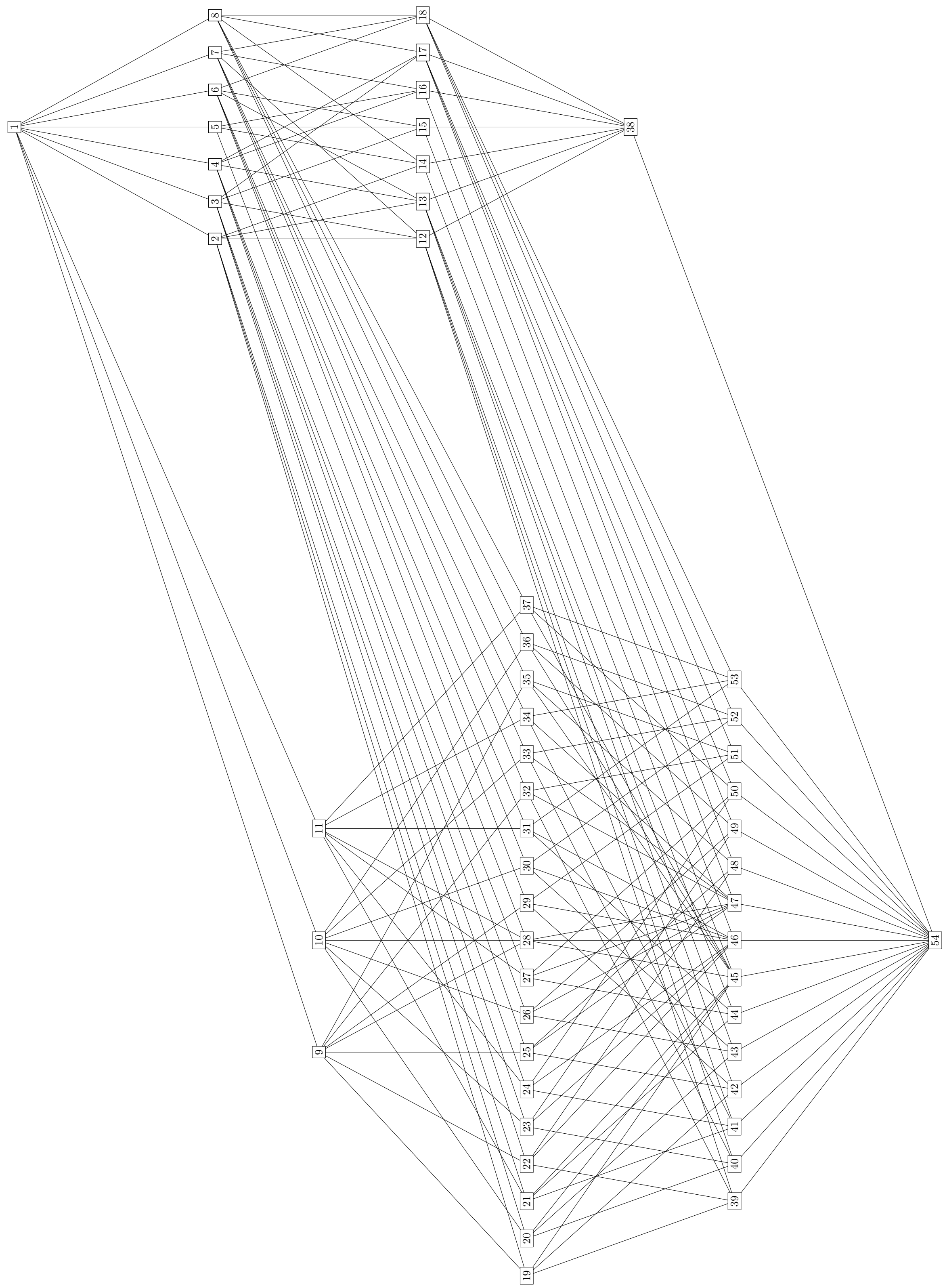

FIGURE 19 – Diagramme de Hasse des sous-groupes de G et des sous-corps de K (en inversant l'ordre)

2 Théorème fondamental

Avant d'énoncer le théorème fondamental de la théorie de Galois, quelques rappels seront utiles. Nous disons qu'un automorphisme σ d'un corps K *fixe* un élément $\alpha \in K$ si $\sigma(\alpha) = \alpha$. Si un tel automorphisme fixe tous les éléments d'un sous-corps F de K, dans ce cas nous disons simplement que σ *fixe* F. Inversement, étant donné un sous-groupe H du groupe $Aut(K)$ des automorphismes de K, le sous-corps de K fixé par tous les automorphismes de ce sous-groupe est dit le corps *laissé fixe* par H. Dans le cas où nous avons une extension de corps K/F, nous notons alors par $Aut(K/F)$ le groupe des automorphismes de K qui fixent F. Cette extension est dite *galoisienne* si son degré $[K : F]$ est fini et égal au cardinal de $Aut(K/F)$. De plus, en supposant l'extension K/F galoisienne, nous identifions $Aut(K/F)$ comme étant le *groupe de Galois* de K/F et nous le notons $Gal(K/F)$.

Cette petite mise en contexte nous amène à énoncer le résultat fondamental suivant.

Théorème 2.1. (Théorème fondamental de la théorie de Galois) *Soit K/F une extension galoisienne et soit $G = Gal(K/F)$. Alors il y a une bijection entre les ensembles suivants :*

$$\{\textit{sous-corps } E \textit{ de } K \textit{ contenant } F\} \longleftrightarrow \{\textit{sous-groupes } H \textit{ de } G\}$$

$$\begin{array}{ccc} K & \longleftrightarrow & \mathbb{I} \\ | & & | \\ E & \longleftrightarrow & H \\ | & & | \\ F & \longleftrightarrow & G \end{array}$$

avec $\mathbb{I} = \{id\}$ où id est l'élément neutre de G. Cette bijection est donnée par les correspondances

$$E \longmapsto \{\textit{les éléments de } G \textit{ qui laissent } E \textit{ fixe}\},$$

$$\{\textit{les éléments du corps laissé fixe par } H\} \longleftarrow\!\shortmid H,$$

qui sont inverses l'une de l'autre. De plus, nous avons les résultats suivants :

(1) Si les corps E_1 et E_2 correspondent respectivement aux groupes H_1 et H_2, alors $E_1 \subseteq E_2$ si et seulement si $H_2 \leq H_1$.

(2) Le degré $[K : E]$ de l'extension K/E est égal à la cardinalité du groupe H associé à E. En d'autres termes, $[K : E] = |H|$. De plus, le degré de l'extension E/F est égal à l'indice du sous-groupe H dans G. En d'autres termes, $[E : F] = [G : H]$:

$$\begin{array}{ll} K & \\ | & \} \ |H| \\ E & \\ | & \} \ |G : H| \\ F & \end{array}$$

(3) L'extension K/E est toujours galoisienne avec $H = Gal(K/E)$ comme groupe de Galois.

(4) L'extension E/F est galoisienne si et seulement si H est un sous-groupe distingué de G. Si c'est le cas, alors le groupe de Galois $Gal(E/F)$ est isomorphe au quotient de groupes G/H.

(5) Si les corps E_1 et E_2 correspondent respectivement aux groupes H_1 et H_2, alors l'intersection $E_1 \cap E_2$ correspond au groupe $\langle H_1, H_2 \rangle$ engendré par H_1 et H_2. De plus, le corps composé E_1E_2 est associé à l'intersection $H_1 \cap H_2$.

3 En quête des sous-corps de $\mathbb{Q}(\omega, \theta, \xi)/\mathbb{Q}$

Par l'intermédiaire du théorème fondamental de la théorie de Galois, nous trouverons la liste des sous-corps de l'extension galoisienne $K/\mathbb{Q}$ où $K = \mathbb{Q}(\omega, \theta, \xi)$. En premier lieu, sachant que le degré de l'extension est 24, nous définirons les automorphismes de K qui forment le groupe de Galois de $K/\mathbb{Q}$. Finalement, nous expliciterons tous les sous-groupes de $G = Gal(K/\mathbb{Q})$ ainsi que tous les sous-corps laissés fixes par ces derniers.

3.1 Automorphismes du groupe de Galois

Tel que susmentionné, l'extension galoisienne est de degré 24. Nous sommes donc à la recherche d'un groupe d'automorphismes ayant ce même nombre d'éléments. La Table 2 explicite les trois générateurs de $Gal(K/\mathbb{Q})$ ainsi que leurs effets sur certains éléments clefs du corps K. Remarquons que $\omega\zeta^2 = \sigma(\omega\zeta) = \sigma(\omega)\sigma(\zeta) = \omega\zeta \cdot \sigma(\zeta)$ de sorte que $\sigma(\zeta) = \zeta$. De plus $\tau(\zeta) = \tau(\frac{1}{2}(1+\theta)) = \frac{1}{2}(1-\theta) = -\left[\frac{1}{2}(1+\theta)\right]^2 = -\zeta^2$.

	ω	$\omega\zeta$	$\omega\zeta^2$	$-\omega$	$-\omega\zeta$	$-\omega\zeta^2$	θ	ξ	ζ
σ	$\omega\zeta$	$\omega\zeta^2$	$-\omega$	$-\omega\zeta$	$-\omega\zeta^2$	ω	θ	ξ	ζ
τ	ω	$-\omega\zeta^2$	$-\omega\zeta$	$-\omega$	$\omega\zeta^2$	$\omega\zeta$	$-\theta$	ξ	$-\zeta^2$
ρ	ω	$\omega\zeta$	$\omega\zeta^2$	$-\omega$	$-\omega\zeta$	$-\omega\zeta^2$	θ	$-\xi$	ζ

TABLE 2 – Table des générateurs σ, τ et ρ de G et leurs effets

Montrons que l'ordre du premier automorphisme σ est 6 et que $\tau\sigma^5 = \sigma\tau$. En effet,

$$\sigma^6(\omega) = \sigma^5(\omega\zeta) = \sigma^4(\omega\zeta^2) = \sigma^3(-\omega) = -\sigma^2(\omega\zeta) = -\sigma(\omega\zeta^2) = w,$$
$$\sigma^6(\theta) = \theta \quad \text{et} \quad \sigma^6(\xi) = \xi,$$
$$\tau\sigma^5(\omega) = \tau\sigma^4(\omega\zeta) = \tau\sigma^3(\omega\zeta^2) = \tau\sigma^2(-\omega) = -\tau\sigma(\omega\zeta) = \omega\zeta = \sigma\tau(\omega),$$
$$\tau\sigma^5(\theta) = \tau(\theta) = -\theta = \sigma(-\theta) = \sigma\tau(\theta) \quad \text{et} \quad \tau\sigma^5(\xi) = \xi = \sigma\tau(\xi).$$

Les deux derniers automorphismes τ et ρ sont en fait d'ordre 2. Nous obtenons donc que le groupe de Galois $G = Gal(K/F) = \langle \sigma, \tau, \rho \rangle$ est isomorphe à $D_{12} \times$

$\mathbb{Z}/2\mathbb{Z}$, où D_{12} est le groupe diédral d'ordre 12. La table de Cayley pour G est représentée dans la Table 3.

3.2 Sous-groupes du groupe de Galois

En vertu du théorème de Lagrange, nous savons que les cardinalités des sous-groupes de G sont des diviseurs de 24. La liste de tous les sous-groupes se trouve dans la colonne appropriée du tableau de la page 78. Selon Neubüser [Neu67], il existe sept groupes de cardinalité 12, trois de cardinalité 8, sept de cardinalité 6, dix-neuf de cardinalité 4, un seul de cardinalité 3 et finalement quinze de cardinalité 2, pour un total de 54 sous-groupes, si nous comptons le groupe lui-même $G = D_{12} \times \mathbb{Z}/2\mathbb{Z}$ et le sous-groupe trivial $\mathbb{I}$.

3.3 Liste des sous-corps

Le cinquième résultat du théorème fondamental donne une méthode efficace pour trouver tous les sous-corps à partir des sous-groupes. L'idée est de commencer avec tous les groupes engendrés par un seul élément (il y en a 18, si nous ignorons le groupe trivial) et de déterminer le sous-corps associé à chacun. Pour ce faire, il faut à prime abord appliquer l'automorphisme générateur à un élément typique de K et nous vérifions quels termes sont fixés.

Par exemple, trouvons le sous-corps associé au groupe $\langle \tau\sigma^4 \rangle$. Un élément typique z de K s'écrit

$$\begin{aligned} z = \quad & a_0 + a_1\omega + a_2\omega^2 + a_3\omega^3 + a_4\omega^4 + a_5\omega^5 \\ & + b_0\theta + b_1\omega\theta + b_2\omega^2\theta + b_3\omega^3\theta + b_4\omega^4\theta + b_5\omega^5\theta \\ & + c_0\xi + c_1\omega\xi + c_2\omega^2\xi + c_3\omega^3\xi + c_4\omega^4\xi + c_5\omega^5\xi \\ & + d_0\theta\xi + d_1\omega\theta\xi + d_2\omega^2\theta\xi + d_3\omega^3\theta\xi + d_4\omega^4\theta\xi + d_5\omega^5\theta\xi. \end{aligned}$$

Par la suite, nous appliquons l'automorphisme $\tau\sigma^4$ sur z :

$$\begin{aligned} \tau\sigma^4(z) = \quad & a_0 - \frac{a_1}{2}\omega(1-\theta) + \frac{a_2}{4}\omega^2(1-\theta)^2 - \frac{a_3}{8}\omega^3(1-\theta)^3 + \frac{a_4}{16}\omega^4(1-\theta)^4 \\ & - \frac{a_5}{32}\omega^5(1-\theta)^5 - b_0\theta + \frac{b_1}{2}\omega(1-\theta)\theta - \frac{b_2}{4}\omega^2(1-\theta)^2\theta \\ & + \frac{b_3}{8}\omega^3(1-\theta)^3\theta - \frac{b_4}{16}\omega^4(1-\theta)^4\theta + \frac{b_5}{32}\omega^5(1-\theta)^5\theta + c_0\theta \\ & - \frac{c_1}{2}\omega(1-\theta)\xi + \frac{c_2}{4}\omega^2(1-\theta)^2\xi - \frac{c_3}{8}\omega^3(1-\theta)^3\xi + \frac{c_4}{16}\omega^4(1-\theta)^4\xi \\ & - \frac{c_5}{32}\omega^5(1-\theta)^5\xi - d_0\theta\xi + \frac{d_1}{2}\omega(1-\theta)\theta\xi - \frac{d_2}{4}\omega^2(1-\theta)^2\theta\xi \\ & + \frac{d_3}{8}\omega^3(1-\theta)^3\theta\xi - \frac{d_4}{16}\omega^4(1-\theta)^4\theta\xi + \frac{d_5}{32}\omega^5(1-\theta)^5\theta\xi \\ = \quad & a_0 - \frac{a_1}{2}\omega(1-\theta) - \frac{a_2}{2}\omega^2(1+\theta) + a_3\omega^3 - \frac{a_4}{2}\omega^4(1-\theta) - \frac{a_5}{2}\omega^5(1+\theta) \\ & - b_0\theta + \frac{b_1}{2}\omega(1-\theta)\theta + \frac{b_2}{2}\omega^2(1+\theta)\theta - b_3\omega^3\theta + \frac{b_4}{2}\omega^4(1-\theta)\theta \\ & + \frac{b_5}{2}\omega^5(1+\theta)\theta + c_0 - \frac{c_1}{2}\omega(1-\theta)\xi - \frac{c_2}{2}\omega^2(1+\theta)\xi + c_3\omega^3\xi \end{aligned}$$

$$
\begin{aligned}
&- \frac{c_4}{2}\omega^4(1-\theta)\xi - \frac{c_5}{2}\omega^5(1+\theta)\xi - d_0\theta\xi + \frac{d_1}{2}\omega(1-\theta)\theta\xi \\
&+ \frac{d_2}{2}\omega^2(1+\theta)\theta\xi - d_3\omega^3\theta\xi + \frac{d_4}{2}\omega^4(1-\theta)\theta\xi + \frac{d_5}{2}\omega^5(1+\theta)\theta\xi \\
= \quad & a_0 + \left(-\frac{a_1}{2} + \frac{3b_1}{2}\right)\omega + \left(-\frac{a_2}{2} - \frac{3b_2}{2}\right)\omega^2 + a_3\omega^3 \\
&+ \left(-\frac{a_4}{2} + \frac{3b_4}{2}\right)\omega^4 + \left(-\frac{a_5}{2} - \frac{3b_5}{2}\right)\omega^5 - b_0\theta + \left(\frac{a_1}{2} + \frac{b_1}{2}\right)\omega\theta \\
&+ \left(-\frac{a_2}{2} + \frac{b_2}{2}\right)\omega^2\theta - b_3\omega^3\theta + \left(\frac{a_4}{2} + \frac{b_4}{2}\right)\omega^4\theta + \left(-\frac{a_5}{2} + \frac{b_5}{2}\right)\omega^5\theta \\
&+ c_0\xi + \left(-\frac{c_1}{2} + \frac{3d_1}{2}\right)\omega\xi + \left(-\frac{c_2}{2} - \frac{3d_2}{2}\right)\omega^2\xi + c_3\omega^3\xi \\
&+ \left(-\frac{c_4}{2} + \frac{3d_4}{2}\right)\omega^4\xi + \left(-\frac{c_5}{2} - \frac{3d_5}{2}\right)\omega^5\xi - d_0\theta\xi + \left(\frac{c_1}{2} + \frac{d_1}{2}\right)\omega\theta\xi \\
&+ \left(-\frac{c_2}{2} + \frac{d_2}{2}\right)\omega^2\theta\xi - d_3\omega^3\theta\xi + \left(\frac{c_4}{2} + \frac{d_4}{2}\right)\omega^4\theta\xi \\
&+ \left(-\frac{c_5}{2} + \frac{d_5}{2}\right)\omega^5\theta\xi.
\end{aligned}
$$

Or, comme nous cherchons le corps laissé fixe par $\langle\tau\sigma^4\rangle$, nous avons $\tau\sigma^4(z) = z$, ce qui entraîne que $b_0 = 0$, $b_1 = a_1$, $b_2 = -a_2$, $b_3 = 0$, $b_4 = a_4$, $b_5 = -a_5$, $d_0 = 0$, $d_1 = c_1$, $d_2 = -c_2$, $d_3 = 0$, $d_4 = c_4$ et $d_5 = -c_5$. Ainsi, z se réduit à

$$
\begin{aligned}
z = \quad & a_0 + a_1\omega(1+\theta) + a_2\omega^2(1-\theta) + a_3\omega^3 + a_4\omega^4(1+\theta) + a_5\omega^5(1-\theta) \\
&+ c_0\xi + c_1\omega(1+\theta)\xi + c_2\omega^2(1-\theta)\xi + c_3\omega^3\xi + c_4\omega^4(1+\theta)\xi \\
&+ c_5\omega^5(1-\theta)\xi \\
= \quad & a_0 + a_1\left(\omega(1+\theta)\right) + a_2'\left(\omega(1+\theta)\right)^2 + a_3'\left(\omega(1+\theta)\right)^3 + a_4'\left(\omega(1+\theta)\right)^4 \\
&+ a_5'\left(\omega(1+\theta)\right)^5 + c_0\xi + c_1\left(\omega(1+\theta)\right)\xi + c_2'\left(\omega(1+\theta)\right)^2\xi \\
&+ c_3'\left(\omega(1+\theta)\right)^3\xi + c_4'\left(\omega(1+\theta)\right)^4\xi + c_5'\left(\omega(1+\theta)\right)^5\xi.
\end{aligned}
$$

Nous pouvons ainsi conclure que comme z est un élément typique de $\mathbb{Q}(\omega(1+\theta),\xi)$, alors ce dernier corps est le corps laissé fixe par $\langle\tau\sigma^4\rangle$.

Après avoir trouvé tous les corps laissés fixes par les groupes cycliques, il ne reste qu'à tenir compte des sous-groupes engendrés par deux automorphismes ou plus. En vertu du cinquième résultat du théorème fondamental de la théorie de Galois, il suffit ensuite de prendre l'intersection des sous-corps qui correspondent aux groupes monogènes qui le composent.

Par exemple, le sous-groupe $\langle\tau\rangle$ correspond au sous-corps $\mathbb{Q}(\omega,\xi)$. En effet, $\tau(\omega) = \omega$, $\tau(\xi) = \xi$ et $|\langle\tau\rangle| = [K : \mathbb{Q}(\omega,\xi)] = 2$, alors le deuxième résultat du théorème nous assure que $\langle\tau\rangle$ ne fixe pas un corps plus grand que $\mathbb{Q}(\omega,\xi)$. De même, le sous-groupe $\langle\sigma\rangle$ est associé à $\mathbb{Q}(\theta,\xi)$, car $\sigma(\theta) = \theta$, $\sigma(\xi) = \xi$ et $\langle\sigma\rangle$ est d'ordre 6, ce qui correspond au degré de $K/\mathbb{Q}(\theta,\xi)$. Nous pouvons donc aisément déduire que le sous-groupe $\langle\tau,\sigma\rangle$ correspond à l'intersection $\mathbb{Q}(\omega,\xi)\cap\mathbb{Q}(\theta,\xi) = \mathbb{Q}(\xi)$.

Il existe des raccourcis pour déterminer les corps laissés fixes par les sous-groupes de G, mais cette technique requiert une bonne intuition et une certaine expérience. À partir d'un sous-groupe donné H, il s'agit de déduire à prime abord un bon candidat pour le corps E, puis de vérifier que les générateurs de H le fixent bel et bien, mais qu'ils ne fixent aucun corps plus grand en comparant l'ordre de H avec le degré de l'extension K/E.

Pour illustrer cette méthode, considérons le groupe $H_{11} = \langle\sigma^3, \tau\sigma, \rho\rangle$. Notre flair nous amène à choisir $E_{11} = \mathbb{Q}(\omega^2(1-\theta))$ comme corps laissé fixe. En premier, nous vérifions les effets des générateurs sur E_{11} :

$$\begin{aligned}
\sigma^3(\omega^2(1-\theta)) = &\quad \left(\sigma^3(\omega)\right)^2 \cdot \sigma^3(1-\theta) = (-\omega)^2\,(1-\theta) = \omega^2(1-\theta),\\
\tau\sigma(\omega^2(1-\theta)) = &\quad (\tau\sigma(\omega))^2 \cdot \tau\sigma(1-\theta) = (\tau(\omega\zeta))^2\,(1+\theta)\\
= &\quad \frac{1}{4}\omega^2(1-\theta)^2(1+\theta) = \omega^2(1-\theta),\\
\rho(\omega^2(1-\theta)) = &\quad \omega^2(1-\theta).
\end{aligned}$$

Les trois générateurs de H_{11} fixent donc E_{11}. Finalement, comme l'ordre de H_{11} vaut 8 et que le degré de K/E_{11} donne également 8, alors le candidat est le bon.

À l'aide de la Table 4, nous pouvons illustrer les relations groupe–sous-groupe ou inversement corps–sous-corps. De plus, le diagramme de Hasse que nous avons exhibé nous donne une vision globale des sous-corps reproduisant le treillis des sous-groupes.

	id	σ	σ^2	σ^3	σ^4	σ^5	τ	$\tau\sigma$	$\tau\sigma^2$	$\tau\sigma^3$	$\tau\sigma^4$	$\tau\sigma^5$	ρ	$\rho\sigma$	$\rho\sigma^2$	$\rho\sigma^3$	$\rho\sigma^4$	$\rho\sigma^5$	$\rho\tau$	$\rho\tau\sigma$	$\rho\tau\sigma^2$	$\rho\tau\sigma^3$	$\rho\tau\sigma^4$	$\rho\tau\sigma^5$
id	id	σ	σ^2	σ^3	σ^4	σ^5	τ	$\tau\sigma$	$\tau\sigma^2$	$\tau\sigma^3$	$\tau\sigma^4$	$\tau\sigma^5$	ρ	$\rho\sigma$	$\rho\sigma^2$	$\rho\sigma^3$	$\rho\sigma^4$	$\rho\sigma^5$	$\rho\tau$	$\rho\tau\sigma$	$\rho\tau\sigma^2$	$\rho\tau\sigma^3$	$\rho\tau\sigma^4$	$\rho\tau\sigma^5$
σ	σ	σ^2	σ^3	σ^4	σ^5	id	$\tau\sigma^5$	τ	$\tau\sigma$	$\tau\sigma^2$	$\tau\sigma^3$	$\tau\sigma^4$	$\rho\sigma$	$\rho\sigma^2$	$\rho\sigma^3$	$\rho\sigma^4$	$\rho\sigma^5$	ρ	$\rho\tau\sigma^5$	$\rho\tau$	$\rho\tau\sigma$	$\rho\tau\sigma^2$	$\rho\tau\sigma^3$	$\rho\tau\sigma^4$
σ^2	σ^2	σ^3	σ^4	σ^5	id	σ	$\tau\sigma^4$	$\tau\sigma^5$	τ	$\tau\sigma$	$\tau\sigma^2$	$\tau\sigma^3$	$\rho\sigma^2$	$\rho\sigma^3$	$\rho\sigma^4$	$\rho\sigma^5$	ρ	$\rho\sigma$	$\rho\tau\sigma^4$	$\rho\tau\sigma^5$	$\rho\tau$	$\rho\tau\sigma$	$\rho\tau\sigma^2$	$\rho\tau\sigma^3$
σ^3	σ^3	σ^4	σ^5	id	σ	σ^2	$\tau\sigma^3$	$\tau\sigma^4$	$\tau\sigma^5$	τ	$\tau\sigma$	$\tau\sigma^2$	$\rho\sigma^3$	$\rho\sigma^4$	$\rho\sigma^5$	ρ	$\rho\sigma$	$\rho\sigma^2$	$\rho\tau\sigma^3$	$\rho\tau\sigma^4$	$\rho\tau\sigma^5$	$\rho\tau$	$\rho\tau\sigma$	$\rho\tau\sigma^2$
σ^4	σ^4	σ^5	id	σ	σ^2	σ^3	$\tau\sigma^2$	$\tau\sigma^3$	$\tau\sigma^4$	$\tau\sigma^5$	τ	$\tau\sigma$	$\rho\sigma^4$	$\rho\sigma^5$	ρ	$\rho\sigma$	$\rho\sigma^2$	$\rho\sigma^3$	$\rho\tau\sigma^2$	$\rho\tau\sigma^3$	$\rho\tau\sigma^4$	$\rho\tau\sigma^5$	$\rho\tau$	$\rho\tau\sigma$
σ^5	σ^5	id	σ	σ^2	σ^3	σ^4	$\tau\sigma$	$\tau\sigma^2$	$\tau\sigma^3$	$\tau\sigma^4$	$\tau\sigma^5$	τ	$\rho\sigma^5$	ρ	$\rho\sigma$	$\rho\sigma^2$	$\rho\sigma^3$	$\rho\sigma^4$	$\rho\tau\sigma$	$\rho\tau\sigma^2$	$\rho\tau\sigma^3$	$\rho\tau\sigma^4$	$\rho\tau\sigma^5$	$\rho\tau$
τ	τ	$\tau\sigma$	$\tau\sigma^2$	$\tau\sigma^3$	$\tau\sigma^4$	$\tau\sigma^5$	id	σ	σ^2	σ^3	σ^4	σ^5	$\rho\tau$	$\rho\tau\sigma$	$\rho\tau\sigma^2$	$\rho\tau\sigma^3$	$\rho\tau\sigma^4$	$\rho\tau\sigma^5$	ρ	$\rho\sigma$	$\rho\sigma^2$	$\rho\sigma^3$	$\rho\sigma^4$	$\rho\sigma^5$
$\tau\sigma$	$\tau\sigma$	$\tau\sigma^2$	$\tau\sigma^3$	$\tau\sigma^4$	$\tau\sigma^5$	τ	σ^5	id	σ	σ^2	σ^3	σ^4	$\rho\tau\sigma$	$\rho\tau\sigma^2$	$\rho\tau\sigma^3$	$\rho\tau\sigma^4$	$\rho\tau\sigma^5$	$\rho\tau$	$\rho\sigma^5$	ρ	$\rho\sigma$	$\rho\sigma^2$	$\rho\sigma^3$	$\rho\sigma^4$
$\tau\sigma^2$	$\tau\sigma^2$	$\tau\sigma^3$	$\tau\sigma^4$	$\tau\sigma^5$	τ	$\tau\sigma$	σ^4	σ^5	id	σ	σ^2	σ^3	$\rho\tau\sigma^2$	$\rho\tau\sigma^3$	$\rho\tau\sigma^4$	$\rho\tau\sigma^5$	$\rho\tau$	$\rho\tau\sigma$	$\rho\sigma^4$	$\rho\sigma^5$	ρ	$\rho\sigma$	$\rho\sigma^2$	$\rho\sigma^3$
$\tau\sigma^3$	$\tau\sigma^3$	$\tau\sigma^4$	$\tau\sigma^5$	τ	$\tau\sigma$	$\tau\sigma^2$	σ^3	σ^4	σ^5	id	σ	σ^2	$\rho\tau\sigma^3$	$\rho\tau\sigma^4$	$\rho\tau\sigma^5$	$\rho\tau$	$\rho\tau\sigma$	$\rho\tau\sigma^2$	$\rho\sigma^3$	$\rho\sigma^4$	$\rho\sigma^5$	ρ	$\rho\sigma$	$\rho\sigma^2$
$\tau\sigma^4$	$\tau\sigma^4$	$\tau\sigma^5$	τ	$\tau\sigma$	$\tau\sigma^2$	$\tau\sigma^3$	σ^2	σ^3	σ^4	σ^5	id	σ	$\rho\tau\sigma^4$	$\rho\tau\sigma^5$	$\rho\tau$	$\rho\tau\sigma$	$\rho\tau\sigma^2$	$\rho\tau\sigma^3$	$\rho\sigma^2$	$\rho\sigma^3$	$\rho\sigma^4$	$\rho\sigma^5$	ρ	$\rho\sigma$
$\tau\sigma^5$	$\tau\sigma^5$	τ	$\tau\sigma$	$\tau\sigma^2$	$\tau\sigma^3$	$\tau\sigma^4$	σ	σ^2	σ^3	σ^4	σ^5	id	$\rho\tau\sigma^5$	$\rho\tau$	$\rho\tau\sigma$	$\rho\tau\sigma^2$	$\rho\tau\sigma^3$	$\rho\tau\sigma^4$	$\rho\sigma$	$\rho\sigma^2$	$\rho\sigma^3$	$\rho\sigma^4$	$\rho\sigma^5$	ρ
ρ	ρ	$\rho\sigma$	$\rho\sigma^2$	$\rho\sigma^3$	$\rho\sigma^4$	$\rho\sigma^5$	$\rho\tau$	$\rho\tau\sigma$	$\rho\tau\sigma^2$	$\rho\tau\sigma^3$	$\rho\tau\sigma^4$	$\rho\tau\sigma^5$	id	$\rho\sigma$	$\rho\sigma^2$	$\rho\sigma^3$	$\rho\sigma^4$	$\rho\sigma^5$	$\rho\tau$	$\rho\tau\sigma$	$\rho\tau\sigma^2$	$\rho\tau\sigma^3$	$\rho\tau\sigma^4$	$\rho\tau\sigma^5$
$\rho\sigma$	$\rho\sigma$	$\rho\sigma^2$	$\rho\sigma^3$	$\rho\sigma^4$	$\rho\sigma^5$	ρ	$\rho\tau\sigma^5$	$\rho\tau$	$\rho\tau\sigma$	$\rho\tau\sigma^2$	$\rho\tau\sigma^3$	$\rho\tau\sigma^4$	σ	σ^2	σ^3	σ^4	σ^5	id	$\tau\sigma^5$	τ	$\tau\sigma$	$\tau\sigma^2$	$\tau\sigma^3$	$\tau\sigma^4$
$\rho\sigma^2$	$\rho\sigma^2$	$\rho\sigma^3$	$\rho\sigma^4$	$\rho\sigma^5$	ρ	$\rho\sigma$	$\rho\tau\sigma^4$	$\rho\tau\sigma^5$	$\rho\tau$	$\rho\tau\sigma$	$\rho\tau\sigma^2$	$\rho\tau\sigma^3$	σ^2	σ^3	σ^4	σ^5	id	σ	$\tau\sigma^4$	$\tau\sigma^5$	τ	$\tau\sigma$	$\tau\sigma^2$	$\tau\sigma^3$
$\rho\sigma^3$	$\rho\sigma^3$	$\rho\sigma^4$	$\rho\sigma^5$	ρ	$\rho\sigma$	$\rho\sigma^2$	$\rho\tau\sigma^3$	$\rho\tau\sigma^4$	$\rho\tau\sigma^5$	$\rho\tau$	$\rho\tau\sigma$	$\rho\tau\sigma^2$	σ^3	σ^4	σ^5	id	σ	σ^2	$\tau\sigma^3$	$\tau\sigma^4$	$\tau\sigma^5$	τ	$\tau\sigma$	$\tau\sigma^2$
$\rho\sigma^4$	$\rho\sigma^4$	$\rho\sigma^5$	ρ	$\rho\sigma$	$\rho\sigma^2$	$\rho\sigma^3$	$\rho\tau\sigma^2$	$\rho\tau\sigma^3$	$\rho\tau\sigma^4$	$\rho\tau\sigma^5$	$\rho\tau$	$\rho\tau\sigma$	σ^4	σ^5	id	σ	σ^2	σ^3	$\tau\sigma^2$	$\tau\sigma^3$	$\tau\sigma^4$	$\tau\sigma^5$	τ	$\tau\sigma$
$\rho\sigma^5$	$\rho\sigma^5$	ρ	$\rho\sigma$	$\rho\sigma^2$	$\rho\sigma^3$	$\rho\sigma^4$	$\rho\tau\sigma$	$\rho\tau\sigma^2$	$\rho\tau\sigma^3$	$\rho\tau\sigma^4$	$\rho\tau\sigma^5$	$\rho\tau$	σ^5	id	σ	σ^2	σ^3	σ^4	$\tau\sigma$	$\tau\sigma^2$	$\tau\sigma^3$	$\tau\sigma^4$	$\tau\sigma^5$	τ
$\rho\tau$	$\rho\tau$	$\rho\tau\sigma$	$\rho\tau\sigma^2$	$\rho\tau\sigma^3$	$\rho\tau\sigma^4$	$\rho\tau\sigma^5$	ρ	$\rho\sigma$	$\rho\sigma^2$	$\rho\sigma^3$	$\rho\sigma^4$	$\rho\sigma^5$	$\rho\rho\tau$	$\tau\sigma$	$\tau\sigma^2$	$\tau\sigma^3$	$\tau\sigma^4$	$\tau\sigma^5$	id	σ	σ^2	σ^3	σ^4	σ^5
$\rho\tau\sigma$	$\rho\tau\sigma$	$\rho\tau\sigma^2$	$\rho\tau\sigma^3$	$\rho\tau\sigma^4$	$\rho\tau\sigma^5$	$\rho\tau$	$\rho\sigma^5$	ρ	$\rho\sigma$	$\rho\sigma^2$	$\rho\sigma^3$	$\rho\sigma^4$	$\tau\sigma$	$\tau\sigma^2$	$\tau\sigma^3$	$\tau\sigma^4$	$\tau\sigma^5$	τ	σ^5	id	σ	σ^2	σ^3	σ^4
$\rho\tau\sigma^2$	$\rho\tau\sigma^2$	$\rho\tau\sigma^3$	$\rho\tau\sigma^4$	$\rho\tau\sigma^5$	$\rho\tau$	$\rho\tau\sigma$	$\rho\sigma^4$	$\rho\sigma^5$	ρ	$\rho\sigma$	$\rho\sigma^2$	$\rho\sigma^3$	$\tau\sigma^2$	$\tau\sigma^3$	$\tau\sigma^4$	$\tau\sigma^5$	τ	$\tau\sigma$	σ^4	σ^5	id	σ	σ^2	σ^3
$\rho\tau\sigma^3$	$\rho\tau\sigma^3$	$\rho\tau\sigma^4$	$\rho\tau\sigma^5$	$\rho\tau$	$\rho\tau\sigma$	$\rho\tau\sigma^2$	$\rho\sigma^3$	$\rho\sigma^4$	$\rho\sigma^5$	ρ	$\rho\sigma$	$\rho\sigma^2$	$\tau\sigma^3$	$\tau\sigma^4$	$\tau\sigma^5$	τ	$\tau\sigma$	$\tau\sigma^2$	σ^3	σ^4	σ^5	id	σ	σ^2
$\rho\tau\sigma^4$	$\rho\tau\sigma^4$	$\rho\tau\sigma^5$	$\rho\tau$	$\rho\tau\sigma$	$\rho\tau\sigma^2$	$\rho\tau\sigma^3$	$\rho\sigma^2$	$\rho\sigma^3$	$\rho\sigma^4$	$\rho\sigma^5$	ρ	$\rho\sigma$	$\tau\sigma^4$	$\tau\sigma^5$	τ	$\tau\sigma$	$\tau\sigma^2$	$\tau\sigma^3$	σ^2	σ^3	σ^4	σ^5	id	σ
$\rho\tau\sigma^5$	$\rho\tau\sigma^5$	$\rho\tau$	$\rho\tau\sigma$	$\rho\tau\sigma^2$	$\rho\tau\sigma^3$	$\rho\tau\sigma^4$	$\rho\sigma$	$\rho\sigma^2$	$\rho\sigma^3$	$\rho\sigma^4$	$\rho\sigma^5$	ρ	$\tau\sigma^5$	τ	$\tau\sigma$	$\tau\sigma^2$	$\tau\sigma^3$	$\tau\sigma^4$	σ	σ^2	σ^3	σ^4	σ^5	id

TABLE 3 – Table de Caylay pour $G = D_{12} \times \mathbb{Z}/2\mathbb{Z}$

n	Sous-groupes	Sous-corps	n	Sous-groupes	Sous-corps
1	$G = \langle \sigma, \tau, \rho \rangle$	$F = \mathbb{Q}$	28	$H_{28} = \langle \sigma^3, \rho \rangle$	$E_{28} = \mathbb{Q}(\omega^2, \theta)$
2	$H_2 = \langle \rho\sigma, \tau \rangle$	$E_2 = \mathbb{Q}(\omega^3 \xi)$	29	$H_{29} = \langle \sigma^3, \rho\tau\sigma^2 \rangle$	$E_{29} = \mathbb{Q}(\omega^2(1+\theta), \theta\xi)$
3	$H_3 = \langle \sigma, \tau \rangle$	$E_3 = \mathbb{Q}(\xi)$	30	$H_{30} = \langle \sigma^3, \rho\tau \rangle$	$E_{30} = \mathbb{Q}(\omega^2, \theta\xi)$
4	$H_4 = \langle \sigma^2, \tau\sigma, \rho \rangle$	$E_4 = \mathbb{Q}(\omega^3 \theta)$	31	$H_{31} = \langle \sigma^3, \rho\tau\sigma \rangle$	$E_{31} = \mathbb{Q}(\omega^2(1-\theta), \theta\xi)$
5	$H_5 = \langle \sigma, \rho \rangle$	$E_5 = \mathbb{Q}(\theta)$	32	$H_{32} = \langle \tau\sigma^2, \rho \rangle$	$E_{32} = \mathbb{Q}(\omega(1-\theta))$
6	$H_6 = \langle \sigma, \rho\tau \rangle$	$E_6 = \mathbb{Q}(\theta\xi)$	33	$H_{33} = \langle \tau, \rho \rangle$	$E_{33} = \mathbb{Q}(\omega)$
7	$H_7 = \langle \sigma^2, \tau, \rho \rangle$	$E_7 = \mathbb{Q}(\omega^3)$	34	$H_{34} = \langle \tau\sigma^4, \rho \rangle$	$E_{34} = \mathbb{Q}(\omega(1+\theta))$
8	$H_8 = \langle \rho\sigma, \rho\tau \rangle$	$E_8 = \mathbb{Q}(\omega^3 \theta\xi)$	35	$H_{35} = \langle \rho\sigma^3, \rho\tau\sigma^2 \rangle$	$E_{35} = \mathbb{Q}(\omega\theta(1-\theta)\xi)$
9	$H_9 = \langle \sigma^3, \tau\sigma^2, \rho \rangle$	$E_9 = \mathbb{Q}(\omega^2(1+\theta))$	36	$H_{36} = \langle \rho\sigma^3, \rho\tau \rangle$	$E_{36} = \mathbb{Q}(\omega\theta\xi)$
10	$H_{10} = \langle \sigma^3, \tau, \rho \rangle$	$E_{10} = \mathbb{Q}(\omega^2)$	37	$H_{37} = \langle \rho\sigma^3, \tau\sigma \rangle$	$E_{37} = \mathbb{Q}(\omega\theta(1+\theta)\xi)$
11	$H_{11} = \langle \sigma^3, \tau\sigma, \rho \rangle$	$E_{11} = \mathbb{Q}(\omega^2(1-\theta))$	38	$H_{38} = \langle \sigma^2 \rangle$	$E_{38} = \mathbb{Q}(\omega^3, \theta, \xi)$
12	$H_{12} = \langle \sigma^2, \tau \rangle$	$E_{12} = \mathbb{Q}(\omega^3, \xi)$	39	$H_{39} = \langle \tau\sigma^2 \rangle$	$E_{39} = \mathbb{Q}(\omega(1-\theta), \xi)$
13	$H_{13} = \langle \sigma^2, \rho\tau\sigma \rangle$	$E_{13} = \mathbb{Q}(\omega^3 \xi, \theta\xi)$	40	$H_{40} = \langle \tau \rangle$	$E_{40} = \mathbb{Q}(\omega, \xi)$
14	$H_{14} = \langle \rho\sigma \rangle$	$E_{14} = \mathbb{Q}(\omega^3 \xi, \theta)$	41	$H_{41} = \langle \tau\sigma^4 \rangle$	$E_{41} = \mathbb{Q}(\omega(1+\theta), \xi)$
15	$H_{15} = \langle \sigma \rangle$	$E_{15} = \mathbb{Q}(\theta, \xi)$	42	$H_{42} = \langle \rho\tau\sigma^5 \rangle$	$E_{42} = \mathbb{Q}(\omega\theta(1-\theta), \theta\xi)$
16	$H_{16} = \langle \sigma^2, \rho \rangle$	$E_{16} = \mathbb{Q}(\omega^3, \theta)$	43	$H_{43} = \langle \rho\tau\sigma^3 \rangle$	$E_{43} = \mathbb{Q}(\omega\theta, \theta\xi)$
17	$H_{17} = \langle \sigma^2, \tau\sigma \rangle$	$E_{17} = \mathbb{Q}(\omega^3 \theta, \xi)$	44	$H_{44} = \langle \rho\tau\sigma \rangle$	$E_{44} = \mathbb{Q}(\omega\theta(1+\theta), \theta\xi)$
18	$H_{18} = \langle \sigma^2, \rho\tau \rangle$	$E_{18} = \mathbb{Q}(\omega^3, \theta\xi)$	45	$H_{45} = \langle \rho\sigma^3 \rangle$	$E_{45} = \mathbb{Q}(\omega\xi, \theta)$
19	$H_{19} = \langle \rho\sigma^3, \tau\sigma^2 \rangle$	$E_{19} = \mathbb{Q}(\omega(1-\theta)\xi)$	46	$H_{46} = \langle \sigma^3 \rangle$	$E_{46} = \mathbb{Q}(\omega^2, \theta, \xi)$
20	$H_{20} = \langle \rho\sigma^3, \tau \rangle$	$E_{20} = \mathbb{Q}(\omega\xi)$	47	$H_{47} = \langle \rho \rangle$	$E_{47} = \mathbb{Q}(\omega, \theta)$
21	$H_{21} = \langle \rho\sigma^3, \tau\sigma^4 \rangle$	$E_{21} = \mathbb{Q}(\omega(1+\theta)\xi)$	48	$H_{48} = \langle \tau\sigma^5 \rangle$	$E_{48} = \mathbb{Q}(\omega\theta(1-\theta), \xi)$
22	$H_{22} = \langle \sigma^3, \tau\sigma^2 \rangle$	$E_{22} = \mathbb{Q}(\omega^2(1+\theta), \xi)$	49	$H_{49} = \langle \tau\sigma^3 \rangle$	$E_{49} = \mathbb{Q}(\omega\theta, \xi)$
23	$H_{23} = \langle \sigma^3, \tau \rangle$	$E_{23} = \mathbb{Q}(\omega^2, \xi)$	50	$H_{50} = \langle \tau\sigma \rangle$	$E_{50} = \mathbb{Q}(\omega\theta(1+\theta), \xi)$
24	$H_{24} = \langle \sigma^3, \tau\sigma \rangle$	$E_{24} = \mathbb{Q}(\omega^2(1-\theta), \xi)$	51	$H_{51} = \langle \rho\tau\sigma^2 \rangle$	$E_{51} = \mathbb{Q}(\omega(1-\theta), \theta\xi)$
25	$H_{25} = \langle \tau\sigma^5, \rho \rangle$	$E_{25} = \mathbb{Q}(\omega\theta(1-\theta))$	52	$H_{52} = \langle \rho\tau \rangle$	$E_{52} = \mathbb{Q}(\omega, \theta\xi)$
26	$H_{26} = \langle \tau\sigma^3, \rho \rangle$	$E_{26} = \mathbb{Q}(\omega\theta)$	53	$H_{53} = \langle \rho\tau\sigma^4 \rangle$	$E_{53} = \mathbb{Q}(\omega(1+\theta), \theta\xi)$
27	$H_{27} = \langle \tau\sigma, \rho \rangle$	$E_{27} = \mathbb{Q}(\omega\theta(1+\theta))$	54	$\mathbb{I}$	$K = \mathbb{Q}(\omega, \theta, \xi)$

TABLE 4 – Liste des sous-groupes et des sous-corps de $\mathbb{Q}(\omega, \theta, \xi)$

4 Conclusion

En fin de compte, l'utilisation du théorème fondamental de la théorie de Galois a été grandement utile dans l'énumération des sous-corps de l'extension algébrique $\mathbb{Q}(\omega, \theta, \xi)/\mathbb{Q}$. Sans la bijection avec les sous-groupes du groupe de Galois, la tâche aurait été impossible. Dans le domaine de la chasse aux groupes de Galois, il existe un document assez important et très intéressant. Il s'agit du mémoire de maîtrise du mathématicien Leonard H. Soicher, qui étudiait alors à l'Université Concordia [Soi81].

Références

[DF04] D. Dummit et R. Foote : *Abstract Algebra*. Wiley, 2004.

[Neu67] J. Neubüser : Die untergruppenverbande der gruppen der ordnungen ≤ 100 mit ausnahme der ordnungen 64 und 96. Habilitationsschrift, Universität Kiel, Kiel, Germany, 1967.

[Soi81] L. Soicher : The computation of galois groups. Mémoire de D.E.A., Concordia University, Montreal, Canada, 1981.

Nicolas Bureau
Département de mathématiques et de statistique, Université Laval
Courriel: nicolas.bureau.2@ulaval.ca